BUREAU
KETENINFORMATISERING
WERK EN INKOMEN

Verantwoordingsrichtlijn 2026

1. Inleiding

Deze Verantwoordingsrichtlijn beschrijft de scope en procedure van verantwoording voor alle partijen die gebruik maken van de GeVS (Gemeenschappelijke elektronische Voorziening Suwi). Volgens het bepaalde in de artikelen 5.22 en 6.4 van de Regeling Suwi moeten UWV, SVB, Colleges van B&W, Bureau Informatie Diensten Nederland (voorheen Inlichtingenbureau) en de op de GeVS aangesloten niet Suwi partijen maatregelen treffen gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensverwerking en zich daarover verantwoorden. Deze verantwoordingsrichtlijn bevat de gezamenlijke afspraken van de Suwi-partijen met betrekking tot de te hanteren normen voor informatiebeveiliging en de wijze waarop partijen verantwoording afleggen over de naleving daarvan. De Verantwoordingsrichtlijn GeVS 2026 vervangt de Verantwoordingsrichtlijn GeVS 2025 vanaf verantwoordingsjaar 2026 en verder en blijft van kracht totdat er een nieuwe Verantwoordingsrichtlijn is. Voor verantwoordingsjaar 2025 geldt dus dat de verantwoordingsrichtlijn 2025 nog van kracht is

De Verantwoordingsrichtlijn GeVS 2026 bestaat uit de volgende onderdelen:

- Doelstelling
- Wijzigingen ten opzichte van de Verantwoordingsrichtlijn GeVS 2025
- Doelgroep voor wie de verplichting geldt
- Een uitwerking van de aanpak
- Bijlage 1: scope van de verantwoording (het uitgewerkte BIO-normenkader)
- Bijlage 2: opmaat naar opzet, bestaan en werking voor gemeenten
- Bijlage 3: formats voor de transparantierapportage.

2. Doelstelling

De Suwi partijen bepalen gezamenlijk het gewenste niveau van informatiebeveiliging voor de GeVS.
Vanaf 1 januari 2020 geldt de Baseline Informatiebeveiliging Overheid (BIO)[1]. De BIO voorziet in een uniform en uitgebreid normenkader informatiebeveiliging voor de gehele overheidssector. Organisaties die de BIO (moeten) implementeren werken daarmee aan het verzekeren van een adequaat niveau van informatiebeveiliging.
Het Ketenoverleg heeft besloten dat vanaf 2020 dit niveau gebaseerd wordt op het normenkader van de BIO en verantwoording op basis daarvan moet plaatsvinden.

[1] Op 23 september 2025 is de BIO 2.0 gepubliceerd. Hierin zullen de normen een andere nummering krijgen. De Verantwoordingsrichtlijn 2026 volgt de BIO 1.04zv nog.

Iedere partij verantwoordt zich in het eigen jaarverslag en levert voor 1 mei van het kalenderjaar volgend op het verantwoordingsjaar een Transparantierapportage op aan BKWI ten behoeve van de Totaalrapportage. Aan de hand van de inhoud van de Totaalrapportage kan beoordeeld worden of de informatiebeveiliging binnen de GeVS adequaat is en of alle afnemers voldoen aan het afgesproken beveiligingsniveau, dat is neergelegd in de specifiek van toepassing zijnde normen uit de BIO.
De beheerders van GeVS (BKWI en BIDN) verantwoorden zich voor 15 maart van het kalenderjaar volgend op het verantwoordingsjaar op het normenkader van de BIO.

3. Wijzigingen t.o.v. de Verantwoordingsrichtlijn GeVS 2025

Vanaf Verantwoordingsjaar 2026 kunnen niet-gemeentelijke afnemers voor hun verantwoording de NOREA audit richtlijnen 3000A of 3000D toepassen. Gemeentelijke afnemers passen NOREA audit richtlijn 3000D toe. Deze aanpassing geeft invulling aan besluitvorming binnen het Strategisch Overleg ENSIA en is doorgevoerd om de eenduidigheid van ENSIA te bewaren,

4. Doelgroep voor wie de verplichting geldt

De goedkeuring en vaststelling van deze Verantwoordingsrichtlijn 2026 in het Managementoverleg Afspraken en Voorzieningen (MAV, voorheen Ketenoverleg) impliceert dat de afnemers die vertegenwoordigd zijn in het MAV gehouden zijn jaarlijks tijdig een transparantierapportage op te leveren zoals beschreven in dit document inclusief bijlagen.
De verantwoordingsplicht is daarnaast ingevolge het Aansluitprotocol van toepassing op andere partijen die gebruik maken van de GeVS, de niet Suwi-partijen. Op deze wijze kan inzicht worden gegeven in het beveiligingsniveau van het gebruik van de Suwinet-services.
De scope van de verantwoording is de beveiligingsmaatregelen van alle gegevensuitwisselingen via de GeVS[2]. Het gaat niet alleen om de services die door de beheerders van de GeVS beschikbaar worden gesteld, maar ook om het gebruik daarvan zowel door applicaties als door medewerkers. Ook wanneer taken zijn uitbesteed aan derden, zoals samenwerkingsverbanden vallen deze onder de verantwoordingsplicht. Datzelfde geldt voor verwerkingen van gegevens voor SUWI-taken en eventueel niet SUWI-taken op verschillende plaatsen in dezelfde organisatie.
Voor de beheerders (BKWI en Bureau Informatie Diensten Nederland) gold tot 2020 een specifiek normenkader voor beheerders dat eveneens is vervangen door de BIO. De verantwoordingsplicht voor beheerders is neergelegd in de SUWI-regeling. De beheerders moeten voor 15 maart van het kalenderjaar volgend op het verantwoordingsjaar de resultaten van een EDP-audit verstrekken aan de minister van SZW, die daardoor adequaat toezicht kan

[2] De instrumentengidsen Dennis & Eva vallen niet onder de Verantwoordingsrichtlijn GeVS.

houden op de informatiebeveiliging bij de beheerders van de GeVS. Deze resultaten maken geen onderdeel uit van de totaalrapportage die in het najaar wordt aangeboden. De verantwoordingsrichtlijn is niet op overeenkomstige wijze van toepassing voor de beheerders.

Afnemers moeten erop toezien dat de GeVS-voorzieningen alleen voor die wetten gebruikt worden zoals genoemd in artikel 62 van de Wet Suwi, art. 5.9 van het besluit Suwi en art. 3.3. Regeling Suwi.

De verantwoordingsplicht geldt expliciet niet voor de levering van gegevens door partijen in hun rol van bronhouder.

De minister van SZW heeft een interventieprotocol opgesteld waarin wordt beschreven hoe SZW zal handelen wanneer niet voldaan wordt aan de verantwoordingsplicht of het niet naleven van het normenkader door gemeenten. Het protocol is van toepassing op alle gemeentelijke- en niet gemeentelijke aansluiters.

5. Aanpak Verantwoording

Transparantie en verantwoording zijn instrumentele functies ten behoeve van de besturing. Transparantie is het bieden van informatie over sturing, implementatie en beheersingsaspecten van de gebruikte Suwinet services en/of DKD.
Verantwoording is een middel om over de mate van “in control zijn” een verklaring af te geven. Met die verklaring verstrekt de Raad van Bestuur van de ZBO aan de Minister van SZW of het College van B&W aan de Gemeenteraad het signaal greep te hebben op de sturing van de dienstverlening en de informatiebeveiliging.
Iedere afnemende partij verantwoordt zich in het eigen jaarverslag en levert voor 1 mei van het kalenderjaar volgend op het verantwoordingsjaar een Transparantierapportage aan BKWI.

Gemeenten
Gemeenten verantwoorden zich vanaf 2017 over informatiebeveiliging volgens de ENSIA-systematiek, die betrekking heeft op de beveiliging van alle gemeentelijke verwerkingen waarbij gebruik wordt gemaakt van de Suwinet services en/of DKD. Berichtenuitwisseling in het kader van ‘WGS plan van aanpak’ en ‘WGS toegang’ vallen onder DKD.
De transparantierapportage bestaat uit:

- Een assurance-rapport volgens de 3000D-methode van een bij de NOREA geregistreerde IT-auditor. Het rapport bevat onder andere een oordeel van de IT-auditor over de mate waarin aan de gestelde normen wordt voldaan en indien van toepassing een overzicht van de normen waaraan niet wordt voldaan.
- Een brief waarmee de gemeentesecretaris het rapport aanbiedt.

BUREAU
KETENINFORMATISERING
WERK EN INKOMEN

Op 1 mei van het jaar na het verantwoordingsjaar moeten de transparantierapportages zijn ontvangen door BKWI via ensia@bkwi.nl of levering via de ENSIA-portal. De afnemende partij is zelf verantwoordelijk voor de aanlevering van de transparantierapportage.
De formats voor de documenten zijn voor gemeenten ook beschikbaar op www.ensia.nl.

Volgens de 'Opmaat voor verantwoording over werking' zoals beschreven in bijlage 2 verantwoorden gemeenten zich vanaf verantwoordingsjaar 2025 over opzet, bestaan en werking. Dit start met een optionele verantwoording op werking over een geselecteerd aantal normen en werkt toe naar een volledige verantwoording over het gehele normenkader in 2027.

Overige afnemers
Voor alle andere partijen (zowel Suwi- als niet Suwi-partijen):
In het geval NOREA richtlijn 3000A wordt gevolgd, bestaat de transparantierapportage uit:

- Een in control verklaring van de bestuurder
- Een bijlage met een overzicht van de normen waaraan (eventueel) niet voldaan wordt
- Een getrouwheidsverklaring van een Register EDP-auditor (assurance-rapport bij de verantwoording).

In het geval NOREA richtlijn 3000D wordt gevolgd, bestaat de transparantierapportage uit:

- Een assurance-rapport volgens de 3000D-methode van een bij de NOREA geregistreerde IT-auditor. Het rapport bevat onder andere een oordeel van de IT-auditor over de mate waarin aan de gestelde normen wordt voldaan en indien van toepassing een overzicht van de normen waaraan niet wordt voldaan.
- Een brief waarmee de bestuurder het rapport aanbiedt.

In bijlage 3 zijn formats opgenomen voor de verantwoordingsdocumenten die horen bij de toepassing van de NOREA richtlijn 3000A.
Voor de getrouwheidsverklaring (3000A) en het rapport van de IT-auditor (3000D) is geen format opgesteld. De NOREA biedt een Handreiking voor de door de auditor uit te voeren werkzaamheden inclusief een format voor de getrouwheidsverklaring / het oordeel en de daarbij behorende bijlage. Wel is het noodzakelijk dat de assurance-rapportage (bij het gebruik van de NOREA richtlijn 3000D) inzicht biedt of bevindingen betrekking hebben op de opzet, bestaan en/of werking van beheersmaatregelen.
Ook is geen format opgenomen voor de aanbiedingsbrief bij het gebruik van de 3000D richtlijn.

Afronding verantwoording

BUREAU
KETENINFORMATISERING
WERK EN INKOMEN

BKWI stelt aan de hand van de verstrekte transparantierapportages een Totaalrapportage op. De Domeingroep Privacy en Beveiliging maakt een toelichting op de bevindingen, trekt conclusies en doet aanbevelingen. De Totaalrapportage wordt voor 1 oktober van het jaar volgend op het verantwoordingsjaar door UWV, SVB en de VNG op bestuurlijk niveau aangeboden aan de Minister van SZW.

Bijlage 1: Scope van de verantwoording: normenkader GeVS

Deze bijlage beschrijft aan welke normen (inclusief de bijbehorende sub-normen) de interne beheersmaatregelen voor de GeVS worden getoetst en waarover gerapporteerd moet worden in de transparantierapportage.

Verantwoording gemeenten:
Gemeenten passen vanaf verantwoordingsjaar 2025 de 'Opmaat naar verantwoording over werking voor gemeenten' toe op de genoemde normen. Over 2026 zullen zeven normen op werking worden getoetst. Over 2027 zullen alle normen op werking worden getoetst.
Verantwoording andere afnemers:
Voor andere afnemers geldt dat voldaan moet worden aan opzet, bestaan en werking van de genoemde normen.

Hoofdstuk	Nummer	Normen
5. Informatiebeveiligingsbeleid	5.1.1	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
5. Informatiebeveiligingsbeleid	5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
6. Organiseren van informatiebeveiliging	6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
6. Organiseren van informatiebeveiliging	6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

7. Veilig personeel	7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
9. Toegangsbeveiliging	9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
9. Toegangsbeveiliging	9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
9. Toegangsbeveiliging	9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
9. Toegangsbeveiliging	9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
10. Cryptografie	10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
12. Beveiliging bedrijfsvoering	12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
12. Beveiliging bedrijfsvoering	12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
12. Beveiliging bedrijfsvoering	12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.

18. Naleving	18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.
12. Beveiliging bedrijfsvoering	12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfs-processen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. Alleen van toepassing bij het gebruik van Suwinet Inlezen of DKD Inlezen.
12. Beveiliging bedrijfsvoering	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen: bedrijfsvoering Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. Alleen van toepassing bij het gebruik van Suwinet Inlezen of DKD Inlezen.

Bijlage 2: Opmaat naar verantwoording over werking voor gemeenten

Gemeenten verantwoorden zich vanaf verantwoordingsjaar 2025 over opzet, bestaan en werking. Hierbij dienen gemeenten zich te houden aan onderstaand schema. Waar de verantwoording over werking ‘optioneel’ is, mag de gemeente op werking laten toetsen, maar is het niet verplicht. Het eerstvolgende jaar nadat toetsing op werking voor een norm optioneel was, zal de toetsing op werking voor die norm verplicht worden.

Norm	Opzet	Bestaan	Werking per 2025	Werking per 2026	Werking per 2027
5.1.1	V	V		O	V
5.1.2	V	V		O	V
6.1.1	V	V		O	V
6.1.2	V	V	O	V	V
7.2.2	V	V	O	V	V
9.2.1	V	V	O	V	V
9.2.2	V	V	O	V	V
9.2.5	V	V	O	V	V
9.2.6	V	V	O	V	V
10.1.1	V	V		O	V
12.1.1	V	V		O	V
12.4.1	V	V	O	V	V
12.4.2	V	V		O	V
18.1.4	V	V		O	V
12.1.2	V	V		O	V
12.1.4	V	V		O	V

V: Verplicht voor gemeenten, O: Optioneel voor gemeenten

BUREAU
KETENINFORMATISERING
WERK EN INKOMEN

Bijlage 3: formats voor de transparantierapportage[3]

Format voor de incontrolverklaring inzake informatiebeveiliging GeVS <jaartal>

Het bestuur van <naam organisatie> geeft met deze verklaring aan in hoeverre <naam organisatie> aan het normenkader GeVS (bijlage 1 van de Verantwoordingsrichtlijn 2026) voor afnemers voldoet.

Reikwijdte verklaring
Deze verklaring betreft de verwerkingen van SUWI-gegevens en het gebruik van ondersteunende ICT-voorzieningen door <naam organisatie>, waarover assurance wordt gevraagd van een Register EDP-auditor. De verklaring omvat het gedurende het verantwoordingsjaar <jaartal> in opzet, bestaan en werking voldoen van de beheersingsmaatregelen aan het normenkader GeVS. De normen zijn geschikt voor het doel van deze verklaring. Deze verklaring is opgesteld ten behoeve van de totaalrapportage die door het ketenoverleg aan de minister van SZW wordt aangeboden.

Verklaring bestuurder
<Indien volledig wordt voldaan de normen: De bestuurder verklaart dat bij <naam organisatie> in voor <jaartal> de beoogde en ingerichte beheersingsmaatregelen voldoen aan het normenkader GeVS.> <Bij uitzonderingen: De bestuurder verklaart dat niet aan alle geselecteerde normen in het normenkader GeVS wordt voldaan. De op de uitzonderingen gerichte beheersmaatregelen zijn in een verbeterplan opgenomen, zijn belegd en worden gemonitord>.

[Plaats, datum] [Bestuurder]

Format voor de bijlage bij de incontrolverklaring inzake informatiebeveiliging GeVS <jaartal>

Deze bijlage is een afzonderlijk onderdeel van de Incontrolverklaring inzake informatiebeveiliging GeVS <jaartal> van <naam organisatie>. Deze verklaring heeft betrekking op het in het verantwoordingsjaar <jaartal> in opzet, bestaan en werking voldoen

[3] Uitsluitend van toepassing wanneer NOREA richtlijn 3000A wordt gevolgd.

van de beheersingsmaatregelen van het normenkader GeVS. Deze bijlage is opgesteld ten behoeve van de totaalrapportage die door het ketenoverleg aan de minister van SZW wordt aangeboden.

Onderwerp van de verklaring is het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS).

Normnaleving

<indien geen afwijkingen van de normen:

Zoals in de bestuurdersverklaring vermeld, voldoen de interne beheersmaatregelen inzake de GeVS voor het verantwoordingsjaar <jaartal> in opzet, bestaan en werking aan alle normen.>

<bij afwijkingen van de normen:

Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de GeVS voor verantwoordingsjaar <jaartal> in opzet, bestaan en werking aan alle normen:

Control/maatregel nummer BIO	Applicatie	Afwijking
…	<Suwinet-Inkijk> of <Suwinet-Inlezen in combinatie met <naam inleesapplicatie>>	<geef aan of de afwijking op opzet, bestaan en/of werking is>

>